

BEST AVAILABLE COPY



1204/892

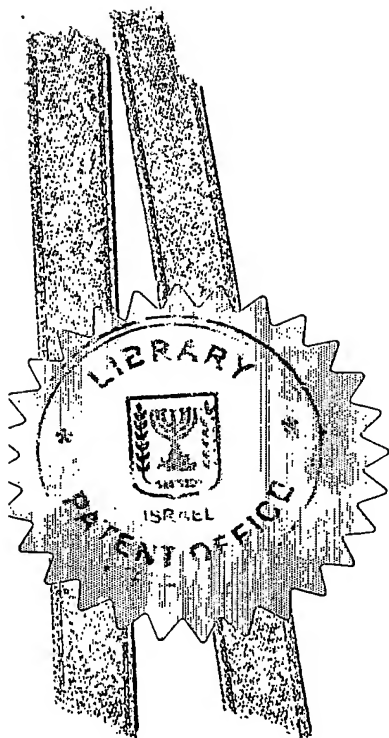
מדינת ישראל
STATE OF ISRAEL

Ministry of Justice
Patent Office

משרד המשפטים
לשכת הפטנטים

This is to certify that
annexed hereto is a true
copy of the documents as
originally deposited with
the patent application
particulars of which are
specified on the first page
of the annex.

זאת לתעודה כי
רצופים בזה העתקים
נכונים של המסמכים
שהופקדו לכתחילה
עם הבקשה לפטנט
לפי הפרטים הרשומים
בעמוד הראשון של
הנספח.



נתאשר
Certified

בקשה לפטנט

Application for Patent

מספר :
158309 :Number

תאריך :
:Date

08-10-2003

הוקדם / נדחה :
:Ante / Post-dated

I (Name and address of applicant, and, in case of body corporate place of incorporation)

Silmarion, Management & Consulting Ltd.
342 Agur Street
Macabim 71918
Israel

סילמריון ניהול ויעוץ בע"מ
רחוב עגור 342
מכבים 71918
ישראל

Inventor: Amnon Yacoby

ממציא: אמנון יעקבי

שמה הוא Law
Of an invention, the title of which is

הדין בעל אמצאה מכח
Owner, by virtue of

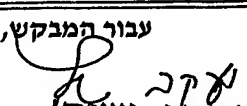
ניהול רשת ממורכז (בעברית)
(Hebrew)

Centralized Network Control

(באנגלית)
(English)

Hereby apply for a patent to be granted to me in respect thereof

מבקש בזאת כי ינתן לי עליה פטנט

*בקשת חלוקה - Application of Division		*בקשת פטנט מוסף - Application for Patent Addition		*דרישה דין קדימה Priority Claim	
מבקשת פטנט from Application No. _____ מס' _____ Dated _____ מיום _____		לבקשה/לפטנט to Patent/Appl. No. _____ מס' _____ Dated _____ מיום _____		מספר/ סימן Number/Mark	תאריך Date
*יפוי כח: כללי/מיוחד - רצוף בזה / עוד יוגש P.O.A: general / individual - attached / to be filed later הוגש בעניין _____ filed in case					
המען למסירת הודעות ומסמכים בישראל Address for Service in Israel פנסטר ושות' קניין רוחני 2002 בע"מ רח' בול 16 פ"ת ת.ד. 10256 פ"ת, 49002					
עבור המבקש,  פנסטר ושות' קניין רוחני 2002 בע"מ		חתימת המבקש Signature of Applicant		שנת 2003 Of the year	בחודש אוקטובר Of
				היום 8 This	לשימוש חלשכה For Office Use

400/03717

טופס זה, כשהוא מוטבע בחותם לשכת הפטנטים ומושלם מספר ובתאריך החגשה, הינו אישור להגשת הבקשה שפרטיה רשומים לעיל.
This form, impressed with the Seal of the Patent Office and indicating the number and date of filing, certifies the filing of the application, the particulars of which are set out above.

Delete whatever is inapplicable *מחס את המיותר

ניהול רשת ממורכז

Centralized Network Control

סילמריון ניהול ויעוץ בע"מ

Silmarion, Management & Consulting Ltd.
c:400/03717

CENTRALIZED NETWORK CONTROL**FIELD OF THE INVENTION**

The present invention relates to computer networks and particularly to control of resource allocation in computer networks.

BACKGROUND OF THE INVENTION

Computer networks are a major work tool in many enterprises and in other organizations. Generally, each user is assigned a computer and a network connects the computers of all the users. The computers may all be located locally and/or may be connected through wide area networks, such as the Internet. The network is used, for example, to exchange data, to access peripherals (e.g., servers, printers) and/or to access databases.

The connection of the computers through a network opens substantially all the resources of the organization to attack. Firewalls are employed at entrance points to the network, in order to protect against attacks and/or penetration attempts launched from computers external to the network. Protecting against an attack or penetration attempt launched from a computer within the network is much more problematic.

Access to a network usually requires entering a user name and password. If the password is determined by eavesdropping, guessing, or using any other method, access to the network may be achieved from substantially any location around the world. In many cases, workers are able to guess and/or determine the passwords of co-workers using methods not related to the computers themselves.

U.S. patent 6,338,138, to Raduchel et al., the disclosure of which is incorporated herein by reference, describes a network based authentication scheme performed in a centralized manner. An authentication manager receives login information and returns indications on the services the user may receive, according to the login information. The user may then download from the authentication manager an applet required to access a service that the user was authorized to access.

U.S. patent 6,088,451, to He et al., the disclosure of which is incorporated herein by reference, describes a method of controlling access to network devices. A user element contacts a network security server and is authenticated by the security server. When the user element wants to open a session with a network device, the user element receives an access ticket and a session encryption key from the security server. The access ticket is encrypted with a password of the network device, such that only the network device can verify the ticket.

Additional unified access management systems are described in U.S. patent 6,460,141, to Olden, and in U.S. patent 6,058,426, the disclosures of which are incorporated herein by reference.

U.S. patent publication 2003/0069972 to Yoshimura et al., the disclosure of which is
5 incorporated herein by reference, describes a network in which virtual local area network (VLAN) definitions are changed dynamically, according to the available bandwidth of the links of the network.

SUMMARY OF THE INVENTION

10 An aspect of some embodiments of the present invention relates to a method of communicating between network elements. Each network element is preconfigured with a plurality of pieces of identification data, e.g., encryption keys and/or functions, which are stored also by a network controller. The pieces of identification data are optionally used for verifying the identity of the network element before the network controller and/or for encrypting network information transmitted between elements of the network.

15 In identity verification, the network controller instructs the network element whose identity is being verified to perform a calculation on one or more, but less than all, the pre-stored pieces of identification data and transmit the result to the controller.

In transmitting network information between entities, one or more, but less than all, the pre-stored pieces of identification data are used in encrypting the information. The receiver of
20 the network information is notified which pieces of the prestored identification data were used in encrypting the network information in the message carrying the encrypted information or in a separate message.

In some embodiments of the invention, the prestored pieces of identification data are used for encrypting information transmitted to and from the network controller. When
25 information is transmitted from the network controller encrypts the information using one or more of the pieces of data stored by the destination network element. The encrypted information is then transmitted to the destination with indication of the identification data pieces to be used in the decryption. In some embodiments of the invention, the encryption additionally uses other keys, for example in accordance with a public-private key.

30 When information is transmitted from the network element to the network controller, the message from the controller instructs the network element which pieces of the identification data to use in the encryption. The transmitted information includes, for example, the status data of the network element.

In some embodiments of the invention, the prestored identification data is used to transmit information between two network elements. The network controller instructs the transmitting network element as to which prestored data pieces to use in the encryption of the information and instructs the receiving element on the data pieces to be used in decrypting the information. Alternatively or additionally, some or all of the network elements perform the tasks described above as performed by the network controller, i.e., selecting the prestored data pieces to be used in the encryption and notifying the destination network element which data pieces are to be used in the decryption or encryption.

Optionally, the prestored pieces of identification data are not transmitted over the network and are only used for calculating the transmitted result, such that the prestored pieces of identification data are kept secret. Using prestored pieces of identification data allows performing simple identity verification procedures and also allows encrypting transmitted network information without requiring agreeing on the key to be used, in a secure manner.

The term network element refers in the present application to any entity belonging to a network including end users (e.g., work stations, personal computers) and network devices (e.g., routers, switches, printers).

In some embodiments of the invention, the data transmission is performed for identity verification purposes and the correct calculation result is known to the network controller. The message from the network controller instructs the network element which identification data pieces to use in the calculation and optionally also provides additional data pieces to be used in the calculation. Optionally, the identity verification is performed for each single network element separately, for example in a sequential manner. Alternatively or additionally, the identity verification may be performed by transmitting a broadcast or multicast transmission and having all receiving elements responding in accordance with the preconfigured pieces of data. Such a multicast transmission may be used to manage an inventory of the elements of the network. Computers not preconfigured with the data pieces will not be able to verify their identity with the controller and therefore will not be able to receive service from the network.

In other embodiments of the invention, the transmitted network information encrypted by one or more pieces of the identification data includes information required for control of the network, such as status information of the network element. Alternatively or additionally, the transmitted information includes commands that control the operation of the network, such as access allowance commands transmitted to network devices (e.g., printers, routers, databases) and/or to network elements of the network.

Optionally, the pieces of identification data include codes belonging to a list of codes prestored in network elements. Optionally, in order not to expose the entire list of codes, only one or two codes are used in each communication between the controller and a network element. In some embodiments of the invention, the codes are never transmitted on the network, but rather are used to encode information being transferred and/or are encrypted by a function. Alternatively or additionally to the pieces of identification data including codes, the pieces of identification data include functions that are to be applied to transferred data and/or to one or more codes. In some embodiments of the invention, less than 10%, 5% or even 2% of the prestored pieces of identification data are used in a single transfer of information and/or in a single identity verification.

In some embodiments of the invention, all the valid network elements are preconfigured with a same set of pieces of identification data. Using the same set of prestored pieces of identification data simplifies secured transmission between network elements not passing through a network controller and/or simplifies the operation of the network controller. Alternatively, different network elements are preconfigured with different pieces of data, for example with different sets of functions. Optionally, at least some encryption calculations involve using both one or more identification data pieces unique to the network element and one or more identification data pieces common to all the valid network elements.

An aspect of some embodiments of the present invention relates to a method of controlling network devices, in which a controller transmits to a network element and to a network device, which the element needs to access, an authentication key that they are to use in communicating with each other. Providing the authentication key to the network device by the controller allows continuous changing of the required authentication key, such that getting hold of an old key does not enable access to the network device.

In some embodiments of the invention, when a network element needs to access a network device, the network element transmits a message to the network controller requesting access permission to the device. The network controller optionally verifies the authenticity of the requesting network element, using any method known in the art and/or as described herein, and provides the network element with a current key of the network device. In some embodiments of the invention, responsive to the request, the controller provides the key to the network device. Alternatively or additionally, the network device is authenticated responsive to the request.

An aspect of some embodiments of the present invention relates to controlling access permission and/or priority to network servers, based on adaptive network parameters. The adaptive network parameters optionally include the location, the connection quality and/or the load of a network element requesting the access. Adapting the access control according to the users resources prevents assigning resources to elements that cannot use the assigned resources and/or to elements that will slow down the operation of the servers.

An aspect of some embodiments of the present invention relates to controlling access permission to network resources, based on adaptive network parameters. The network resources optionally include network servers and/or routers.

There is therefore provided in accordance with an exemplary embodiment of the invention, a method of communicating within a network, comprising configuring a network element with a plurality of pieces of identification data, unique to the network to which the network element belongs, transmitting from a network controller to the network element an instruction to perform a calculation using at least one piece, but not all, of the configured pieces of identification data, and performing the instructed calculation by the network element responsive to the instruction.

Optionally, substantially all the network elements of the network are configured with the same plurality of pieces of identification data. Optionally, different of the network elements of the network are configured with different sets of plurality of pieces of identification data. Optionally, the plurality of pieces of identification data comprise a plurality of codes. Optionally, the plurality of codes have a sequential order and the instruction identifies the codes by a number identifying their order in the sequence.

Optionally, the plurality of pieces of identification data comprise a plurality of functions. Optionally, transmitting the instruction comprises transmitting an instruction to use less than 5% of the configured pieces of identification data. Optionally, transmitting the instruction comprises transmitting an instruction to use a single piece of the configured pieces of identification data. Optionally, transmitting the instruction comprises transmitting an instruction to use in the calculation a single code and a single function of the configured pieces of identification data. Optionally, the method includes transmitting a result of the calculation to the network controller. Optionally, the method includes verifying by the controller that the transmitted result of the calculation is equal to a predetermined value indicative that the network element is part of a network controlled by the controller.

Optionally, the method includes performing by the controller a reverse calculation on the transmitted result of the calculation so as to extract information transmitted from the network element to the controller. Optionally, the extracted transmitted information comprises information on the status of the network element. Optionally, a result of the calculation
5 includes information transferred from the controller to the network element. Optionally, the information transferred from the controller to the network element comprises an instruction on access permissions to be given by the network element.

Optionally, the information transferred from the controller to the network element comprises a code to be given by a different network element accessing the network element
10 receiving the transferred information. Optionally, transmitting the instruction from the network controller comprises transmitting a unicast packet. Optionally, transmitting the instruction from the network controller comprises transmitting a multicast packet. Optionally, the multicast packet requires that all the elements of the network perform a same calculation.

There is further provided in accordance with an exemplary embodiment of the
15 invention, a method of controlling resource access within a network, comprising transmitting by a network element a request to use a resource of a network device, transmitting, by a controller to the network device, a message indicating a code required from the network element in order to access the network device and allowing the network element to use the resource if the required code is received from the network element.

20 Optionally, transmitting the request comprises transmitting from the network element to the network device and forwarding from the network device to the controller.

Optionally, transmitting the request comprises transmitting from the network element directly to the controller. Optionally, transmitting the message indicating the code comprises transmitting a message indicating a calculation to be performed on data configured in the
25 network device in order to extract the code. Optionally, the method includes transmitting a message indicating the required code from the controller to the network element. Optionally, the messages to the network device and to the network element indicate substantially identical calculations to be performed in order to determine the code. Optionally, the messages to the network device and to the network element indicate different calculations to be performed in
30 order to determine the code.

There is further provided in accordance with an exemplary embodiment of the invention, a method of controlling resource access within a network, comprising determining a network condition of a network element and assigning the network element an access priority

to be provided by a network server, at least partially based on the determined network condition. Optionally, the network condition comprises a location of the network element.

Optionally, the network condition comprises a bandwidth or quality of a connection of the network element to the network.

5 There is further provided in accordance with an exemplary embodiment of the invention, a method of controlling resource access within a network, comprising determining a network condition of a network element and assigning the network element an access permission to a network device, at least partially based on the determined network condition.

BRIEF DESCRIPTION OF THE DRAWINGS

10 Exemplary non-limiting embodiments of the invention will be described with reference to the following description of the embodiments, in conjunction with the figures. Identical structures, elements or parts which appear in more than one figure are preferably labeled with a same or similar number in all the figures in which they appear, and in which:

Fig. 1 is a schematic illustration of a computer network, in accordance with an
15 exemplary embodiment of the present invention;

Fig. 2 is a schematic illustration of data exchanged in authenticating a network element, in accordance with an exemplary embodiment of the invention;

Fig. 3 is a schematic illustration of collecting data from a network element, in accordance with an exemplary embodiment of the invention;

20 Fig. 4 is a schematic illustration of transmitting data from a controller to a network element, in accordance with an exemplary embodiment of the invention; and

Fig. 5 is a schematic illustration of a procedure of requesting service from a network device, in accordance with an exemplary embodiment of the invention.

DETAILED DESCRIPTION OF EXEMPLARY EMBODIMENTS

25 Fig. 1 is a schematic illustration of a computer network 100, in accordance with an exemplary embodiment of the present invention. Network 100 optionally includes a plurality of end-users 102 connected through routers 106 and/or switches 108. Some end-users 102 may be connected to network 100 through an external network 120, such as the Internet. End users 102 may be connected to the network through wire links (e.g., dial up connections, Ethernet
30 cables) or through wireless links. The end-users 102 may connect to the network from the same point at all times, or may connect from different points at different times. For example, some or all of end-users 102 may include laptops or PDAs that connect from home using a dialup or ADSL connection and at the office through a local area network (LAN) connection.

Network 100 optionally further comprises network devices, such as a printer 104 and servers 110 that provide services to end-users 102. Servers 110 may include, for example, access application servers, such as ERP and CRM servers, database servers, outlook exchange servers and any other types of servers known in the art. Although not shown, network 100 may include substantially any other additional devices or apparatus known in the art, such as load balancers.

The term network device refers in the present application to any device belonging to the network that is not an end-user, i.e., that services other network elements. The network devices include, for example, printers 104, switches 108, routers 106 and servers 110. The term network element refers in the present application to any entity belonging to the network including end users 102 and network devices.

A network controller 125 keeps track of the elements of network 100 and controls the access permissions to the network devices. Performing both the tracking of the elements of the network and the control of the access permissions from a single point allows using the same control packets for both tasks. In addition, the combined performance of the tasks allows easy control by a human operator. It is noted, however, that the invention also encompasses using controllers 125 that perform only one of the tasks, in a network having two different controllers, in a network having one of the tasks using methods known in the art or in a network in which only one of the tasks is performed.

Each network element is configured with a code vector formed of a plurality of code portions. The code vector is optionally the same for all the network elements. In addition, each network element is configured with a separate unique code keyID. In some embodiments of the invention, each network element is configured with a list of functions $h_i()$ for use in transferring data between controller 125 and the network elements, as described below. Functions $h_i()$ are optionally reversible so that the transferred data can be extracted by using the reverse function. Optionally, in transferring data, the controller selects one of the functions and/or one of the vector portions arbitrarily, so as to reduce the chances that an eavesdropper will be able to guess the code portion and/or the function. The controller then notifies the network element with which it communicates on the index of the vector portion it selected for the transmission.

In an exemplary embodiment of the invention, each element is configured with a sufficient number of code portions and/or functions, so that determination of the code vector

and/or the functions from listening to the network is very difficult. Optionally, the number of functions and/or code portions used are limited according to the resources of the network elements. In an exemplary embodiment of the invention, each network element is configured with 64 functions and the code vector includes 128 code portions. Optionally, the functions $h()$ are relatively simple functions, for example based on logical operations (e.g., and, or) that do not require substantial amounts of processing resources. In accordance with the present invention, high protection levels are achieved, without using complex encryption functions that are processing power intensive.

In some embodiments of the invention, all network elements are configured with the same list of functions $h_i()$. Alternatively, each network element is configured with a different list of functions or each group of network elements is configured with a separate list of functions. For example, each type of network device (e.g., printers, servers) may be configured with a separate list of functions. Alternatively, randomly selected groups may be configured with different lists of functions. Controller 125 is configured with the code vector, the function lists and the unique code of each network element.

In some embodiments of the invention, each network element is initially configured manually by a human system operator. Alternatively, controller 125 is given a list of the network elements belonging to the network and it automatically configures each of the network elements.

Fig. 2 is a schematic illustration of data exchanged in authenticating a network element (e.g., end user 102, server 110) by controller 125, in accordance with an exemplary embodiment of the invention. When required to authenticate the identity of a network element, controller 125 optionally transmits (200) to the network element an index i of a portion of code vector S_i to be used and a function to be applied to the code vector portion S_i . The network element transmits (202) back to controller 125 the result $f(S_i)$ of applying the function $f()$ to S_i . Controller 125 verifies that the result $f(S_i)$ returned from the network element is correct. In some embodiments of the invention, controller 125 additionally transmits (204) to the network element a function $g()$ and index j . The network element applies function $g()$ to its unique code keyID and to the portion j of the common code vector S . The result $g(\text{keyID}, S_j)$ is returned (206) to controller 125, which verifies the correctness of the result.

Transmitting the function $f()$ to the network element, rather than using a function already stored in the network element, prevents the possibility of pre-configuring a network

element, which does not have the code vector, with the result of applying preconfigured functions on code portions, for example as determined from listening to traffic on the network.

A computer not configured with the vector code S cannot return the correct results as it does not have vector S . It is noted that S cannot be determined from listening to the network, since $S_{i,j}$ are not transmitted on the network. Optionally, functions $f()$ and/or $g(.)$ do not allow simple reverse determination of $S_{i,j}$, from the results transmitted on the network. In some embodiments of the invention, functions $f()$ and/or $g(.)$ do not allow determination of $S_{i,j}$ at all, for example due to the functions generating the same value for a plurality of different possible values S_i . Alternatively or additionally, functions $f()$ and/or $g(.)$ are not transmitted to the network element. Instead, each network element is configured with a list of functions $\{f_k\}$ and/or $g(.)$ and controller 125 transmits (200) to the network element an index k of the function to be used.

Alternatively to transmitting functions $f()$ and $g(.)$ separately to the network element, the functions are transmitted to the network element together in a single message. Optionally, in this alternative, the network element responds with both results in the same message. The authenticating method of Fig. 2 is optionally performed periodically. In some embodiments of the invention, the authentication is performed with each network element separately. Alternatively or additionally, controller 125 periodically transmits a multicast or broadcast authenticating message requesting that all the network elements respond. Optionally, the network elements respond at random intervals, in order to distribute the load of the responses. According to the responses, controller 125 optionally generates periodic reports of the network elements currently connected to the network. Alternatively or additionally, authentication is performed whenever it is desired to transmit commands and/or information to a network element and/or to receive information from a network element.

Computers and/or other processors connected to the network that do not have the configured code of the network will not be able to be authenticated by network server 125. As described below, in some embodiments of the invention, the access to network devices, including switches and/or routers, requires receiving an access key from controller 125. Therefore, the computers and/or other processors that do not belong to the network will not be able to communicate with other elements of the network.

Fig. 3 is a schematic illustration of collecting data from a network element 150 by controller 125, in accordance with an exemplary embodiment of the invention. Controller 125

optionally instructs (300) the network element to calculate $f(S_i)$ for a given i , and $g(\text{keyID}, S_j)$ for a given j , as described above with reference to Fig. 2. In addition, controller 125 transmits (302) to network element 150 an indication m of a prestored function h to be used in encoding the collected data. Optionally, controller 125 further provides (304) an indication of the data requested by controller 125. Alternatively, only a single type of data is collected (for example, a vector including all the data possibly of interest), so that an indication of the type of data is not required.

Network element 150 responds (306) with $h\{f(S_i), g(\text{keyID}, S_j), \text{DAT}\}$, wherein DAT is the requested data. Controller 125 then extracts the data DAT by reversing the operation of function h .

In an exemplary embodiment of the invention, the collected data DAT includes a status vector of network element 150 and its surroundings. Optionally, the status vector states the connection bandwidth and/or quality of each connection to network element 150. Alternatively or additionally, the status vector states the amount of data transmitted/received on the connections of network element 150. Further alternatively or additionally, the status vector states the applications, servers and/or other network elements that recently communicated with the network element 150.

In some embodiments of the invention, the collected data includes the location of the end-users 102 or of all the network elements. Optionally, each end-user 102 determines the IP address and/or other identity information of its adjacent routers and provides the IP address as the location information. In some embodiments of the invention, routers and/or switches of the network report their neighboring end-users 102 and the data is compared to verify correctness. Alternatively, for simplicity, location information of end-users 102 is provided only by the routers and/or switches of the network. According to the location information received from the network elements, controller 125 optionally generates and/or updates a map of the network.

Fig. 4 is a schematic illustration of transmitting data from controller 125 to a network element 150, in accordance with an exemplary embodiment of the invention. Controller 125 optionally instructs (400) the network element to calculate $f(S_i)$ for a given i , and $g(\text{keyID}, S_j)$ for a given j , as described above with reference to Fig. 2. In addition, controller 125 transmits (402) to the network element an encoded form (ENC) of the transmitted data and an indication m of a function h to be applied to the encoded transmitted data (ENC) and to $f(S_i)$ and $g(\text{keyID}, S_j)$ in order to extract the transmitted data $h\{f(S_i), g(\text{keyID}, S_j), \text{ENC}\}$. Using this

method, a network element not belonging to the network (i.e., not having the configured code vector S), or not having the unique keyID of the destination, will not be able to decipher the transmitted data.

Optionally, in this embodiment, $f(S_i)$ and $g(\text{keyID}, S_j)$ are not transmitted separately, so that it is harder for an eavesdropper to determine the transmitted data. Alternatively, the data transmission is performed following an authentication procedure as described with reference to Fig. 2, and in order to minimize the load on network 100, $f(S_i)$ and $g(\text{keyID}, S_j)$ from the authentication procedure are used in the data transmission.

In some embodiments of the invention, controller 125 selects the indices i, j and/or the function $h()$ so that it is possible to use the result of function $h()$ for data transfer. Alternatively, ENC is sufficiently large, so that any desired data can be encoded with substantially any code portions and/or function $h()$.

In an exemplary embodiment of the invention, the transmitted data comprises an access vector provided to an end-user 102. For example, the access vector may include a bit for each network device of network 100. A bit which is set indicates that the end-user 102 may access the device corresponding to the set bit. Alternatively or additionally, one or more devices are represented by a plurality of bits, which indicate, for example, the priority of the end-user in accessing the respective device. In some embodiments of the invention, in determining the access vector, network element 150 performs a logical operation between the resultant value $h\{f(S_i), g(\text{keyID}, S_j), \text{ENC}\}$ and a locally determined access vector, which indicates devices not to be accessed or to be given low priority due to preferences of network element 150 and/or environmental conditions. The environmental conditions optionally include a determination of whether the end-user 102 is within the network or outside the network, as determined for example according to whether its packets pass through a firewall and/or an external port of the network. Alternatively or additionally, the environmental conditions include the speed and/or bandwidth of the connection of end-user 102 with the network and/or the quality of the connection as indicated by the percentage of lost packets, the BER and/or any other suitable quality measure.

Optionally, each end-user 102 manages an access vector which states the permissions for the end-user to access each of the network devices. Optionally, the access vector is updated each time an access vector update message is received from controller 125 and/or each time the environmental conditions change.

In another exemplary embodiment of the invention, the transmitted data comprises access allowance instructions provided to a network device (e.g., a server 110). Optionally, in accordance with this exemplary embodiment, the transmitted data includes an identification number of an end-user 102 and a respective access priority of the end-user. In some
5 embodiments of the invention, the transmitted data includes a list of end user identification numbers and respective access priorities. Optionally, in addition to the access priority, the transmitted data includes for each end-user 102 an access code which is to be provided by the end user when it approaches the network device for service.

Fig. 5 is a schematic illustration of a procedure of requesting service from a network
10 device 180, in accordance with an exemplary embodiment of the invention. As described above with reference to Fig. 4, controller 125 transmits (500) to network device 180 a list that states, for each end user 102, an access code to be received from the end-user. Optionally, controller 125 also transmits (502) to end user 102 the access code it is to provide to network device 180. Thereafter, end user 102 transmits (504) a service request including its
15 identification and the access code to network device 180. Using this method prevents end users 102 from receiving service from network devices 180, without registering first with controller 125.

In some embodiments of the invention, the access code is determined separately, for each service request, such that end users 102 cannot use old access codes and/or access codes
20 assigned to other network elements. Alternatively or additionally, the access codes are changed periodically. Optionally, the access codes are changed even when a connection is in progress, in which case, the end user 102 needs to transmit the new access code to the network device within a predetermined time in order to prevent the connection from shutting down. Alternatively, changes in the access codes only affect new connections.

25 In some embodiments of the invention, the access code is provided at the beginning of each connection in a connection establishment stage. Alternatively or additionally, the access code is provided in each packet of the connection, in a field designated therefore.

The transmission (500) to network device 180 of the access codes and priorities of the end users 102 is optionally performed without relation to requests of end users 102 for service.
30 In some embodiments of the invention, the transmission (500) of access codes and priorities is performed periodically, for example every 10-20 minutes, although any other longer or shorter periods may be used. Alternatively or additionally, the transmission (500) of access codes and/or priorities is performed whenever there is a change in the priorities and/or access rights

of an end user 102. Optionally, the transmission (502) of access codes to end-users 102 is also performed without relation to requests for service.

As mentioned above, in some embodiments of the invention, the access codes are generated and/or transmitted responsive to a request for service of end-user 102. Optionally, end-user 102 transmits the request for service directly to controller 125. Responsive to the request, controller 125 provides end-user 102 with an access code. End-user 102 then uses the access code to directly approach network device 180. In some embodiments of the invention, controller 125 generates the access code responsive to the request of end-user 102. Alternatively, controller 125 provides end-user 102, responsive to the request, a pre-generated code, optionally a code already transmitted to network device 180.

Alternatively to transmitting the request to controller 125, the request is transmitted directly to network device 180. Network device 180 forwards the request to controller 125 which provides the access codes to end-user 102 and if necessary to network device 180. Optionally, along with the request, network device 180 notifies controller 125 whether it requires an access code.

Alternatively to transmitting the code itself from end-user 102 to network device 180, the end-user transmits instructions to be performed on the configured code in order to extract the code. Thus, the code can be used for a longer period as it is not exposed on the network.

In some embodiments of the invention, some or all of the routers and/or switches of network 100 are controlled in accordance with the method of Fig. 5. These routers and/or servers examine each packet passing through them for security. Optionally, packets belonging to an existing session are forwarded by the router if their session was registered by the router. New sessions are optionally established only if an ID as required by controller 125 is provided. Alternatively or additionally, all the packets of the session are required to carry the ID required by controller 125. In some embodiments of the invention, packets directed to specific ports that do not involve a security hazard, such as non-hazardous packets (for example packets known to have passed through a firewall) directed to e-mail ports, are allowed to pass even if they are from computers not belonging to the network, so that communication with the external world is not prevented.

Computers not belonging to the network will not be able to communicate through the network. Even if a computer is connected to a LAN or other connection within the network, the computer will not be able to communicate with any other elements of the network. The routers optionally additionally make logs of packets that do not carry the required codes, so

that a human operator will be able to track attempts to penetrate and/or attack the network, and/or to identify computers that are illegitimately connected to the network.

As described above, in some embodiments of the invention, the access permissions of end-users 102 may be adjusted according to their environmental conditions. For example, end-users having a low bandwidth connection to the network may be provided lower priority on a database that provides large amounts of data. In some embodiments of the invention, each end-user is required to adjust its access permissions on its own according to its environment conditions. Alternatively, end-users 102 report their environmental conditions to controller 125 which determines the priority and/or access permissions of the users accordingly. In some embodiments of the invention, the environmental conditions are verified or determined using information from neighboring network elements. Although more complex, in accordance with these embodiments it is much harder for users to fiddle with the environment conditions in order to receive permissions they do not deserve.

In an exemplary embodiment of the invention, a user connected from home is not allowed to use printers that are highly loaded or is not allowed to use printers at all. Alternatively, jobs of users at home are given low priority. Alternatively or additionally, for security reasons, users are not allowed to use certain applications unless they are located within a specific physical location or using a specific computer. In some embodiments of the invention, the maximal size of files that an end-user is allowed to transfer is set according to the bandwidth of the connection of the end-user to the network. Alternatively or additionally, users having a low quality connection are not allowed to access databases that are sensitive to errors which may affect their updating.

In the above description, each network element is configured with both codes and functions. It is noted, however, that the invention may be implemented, although with less security, without configuring the network elements with lists of functions. Instead, controller 125 may transmit the functions used to the network elements each time a function is to be used. Alternatively, the network elements may be configured with sets of functions, and the numbers to which the selected functions are applied are transmitted to the network elements by controller 125.

In some embodiments of the invention, in addition to the protection provided using preconfigured data, passwords are required so that an unauthorized user of a computer belonging to the network will have to overcome the password barrier. Optionally, the permissions allowed to a user depend on both the user login and the computer used. For

example, a user logging in from a computer which is not the regular computer of the user may be limited to specific simple tasks. Similarly, a computer may be allocated different priorities according to the login of the human user of the computer.

5 It will be appreciated that the above-described methods may be varied in many ways, including, changing the order of steps, and/or performing a plurality of steps concurrently. For example, data described as being transmitted in different acts may be transmitted together in a single packet and data described as being transmitted in a single act may be transmitted in a plurality of packets. It should also be appreciated that the above described description of methods and apparatus are to be interpreted as including apparatus for carrying out the
10 methods, and methods of using the apparatus.

The present invention has been described using non-limiting detailed descriptions of embodiments thereof that are provided by way of example and are not intended to limit the scope of the invention. It should be understood that features and/or steps described with respect to one embodiment may be used with other embodiments and that not all embodiments
15 of the invention have all of the features and/or steps shown in a particular figure or described with respect to one of the embodiments. Variations of embodiments described will occur to persons of the art. Furthermore, the terms "comprise," "include," "have" and their conjugates, shall mean, when used in the claims, "including but not necessarily limited to."

It is noted that some of the above described embodiments may describe the best mode
20 contemplated by the inventors and therefore may include structure, acts or details of structures and acts that may not be essential to the invention and which are described as examples. Structure and acts described herein are replaceable by equivalents which perform the same function, even if the structure or acts are different, as known in the art. Therefore, the scope of the invention is limited only by the elements and limitations as used in the claims.

CLAIMS

1. A method of communicating within a network, comprising:
configuring a network element with a plurality of pieces of identification data, unique
5 to the network to which the network element belongs;
transmitting from a network controller to the network element an instruction to
perform a calculation using at least one piece, but not all, of the configured pieces of
identification data; and
performing the instructed calculation by the network element responsive to the
10 instruction.
2. A method according to claim 1, wherein substantially all the network elements of the
network are configured with the same plurality of pieces of identification data.
- 15 3. A method according to claim 1, wherein different of the network elements of the
network are configured with different sets of plurality of pieces of identification data.
4. A method according to any of the preceding claims, wherein the plurality of pieces of
identification data comprise a plurality of codes.
20
5. A method according to claim 4, wherein the plurality of codes have a sequential order
and the instruction identifies the codes by a number identifying their order in the sequence.
6. A method according to any of the preceding claims, wherein the plurality of pieces of
25 identification data comprise a plurality of functions.
7. A method according to any of the preceding claims, wherein transmitting the
instruction comprises transmitting an instruction to use less than 5% of the configured pieces
of identification data.
30
8. A method according to claim 7, wherein transmitting the instruction comprises
transmitting an instruction to use a single piece of the configured pieces of identification data.

9. A method according to claim 7, wherein transmitting the instruction comprises transmitting an instruction to use in the calculation a single code and a single function of the configured pieces of identification data.
- 5 10. A method according to any of the preceding claims, comprising transmitting a result of the calculation to the network controller.
11. A method according to claim 10, comprising verifying by the controller that the transmitted result of the calculation is equal to a predetermined value indicative that the
10 network element is part of a network controlled by the controller.
12. A method according to claim 10, comprising performing by the controller a reverse calculation on the transmitted result of the calculation so as to extract information transmitted from the network element to the controller.
- 15 13. A method according to claim 12, wherein the extracted transmitted information comprises information on the status of the network element.
14. A method according to any of the preceding claims, wherein a result of the calculation
20 includes information transferred from the controller to the network element.
15. A method according to claim 14, wherein the information transferred from the controller to the network element comprises an instruction on access permissions to be given by the network element.
- 25 16. A method according to claim 14, wherein the information transferred from the controller to the network element comprises a code to be given by a different network element accessing the network element receiving the transferred information.
- 30 17. A method according to any of the preceding claims, wherein transmitting the instruction from the network controller comprises transmitting a unicast packet.

18. A method according to any of the preceding claims, wherein transmitting the instruction from the network controller comprises transmitting a multicast packet.

19. A method according to claim 18, wherein the multicast packet requires that all the
5 elements of the network perform a same calculation.

20. A method of controlling resource access within a network, comprising:
transmitting by a network element a request to use a resource of a network device;
transmitting, by a controller to the network device, a message indicating a code
10 required from the network element in order to access the network device; and
allowing the network element to use the resource if the required code is received from
the network element.

21. A method according to claim 20, wherein transmitting the request comprises
15 transmitting from the network element to the network device and forwarding from the network
device to the controller.

22. A method according to claim 20, wherein transmitting the request comprises
transmitting from the network element directly to the controller.
20

23. A method according to claim 20, wherein transmitting the message indicating the code
comprises transmitting a message indicating a calculation to be performed on data configured
in the network device in order to extract the code.

24. A method according to claim 20, comprising transmitting a message indicating the
25 required code from the controller to the network element.

25. A method according to claim 24, wherein the messages to the network device and to
the network element indicate substantially identical calculations to be performed in order to
30 determine the code.

26. A method according to claim 24, wherein the messages to the network device and to the network element indicate different calculations to be performed in order to determine the code.

5 27. A method of controlling resource access within a network, comprising:
determining a network condition of a network element; and
assigning the network element an access priority to be provided by a network server, at least partially based on the determined network condition.

10 28. A method according to claim 27, wherein the network condition comprises a location of the network element.

29. A method according to claim 27, wherein the network condition comprises a bandwidth or quality of a connection of the network element to the network.

15 30. A method of controlling resource access within a network, comprising:
determining a network condition of a network element; and
assigning the network element an access permission to a network device, at least partially based on the determined network condition.

20

For the applicant,



Fenster & Co. Intellectual
Property 2002, Ltd.
c:400/03717

25

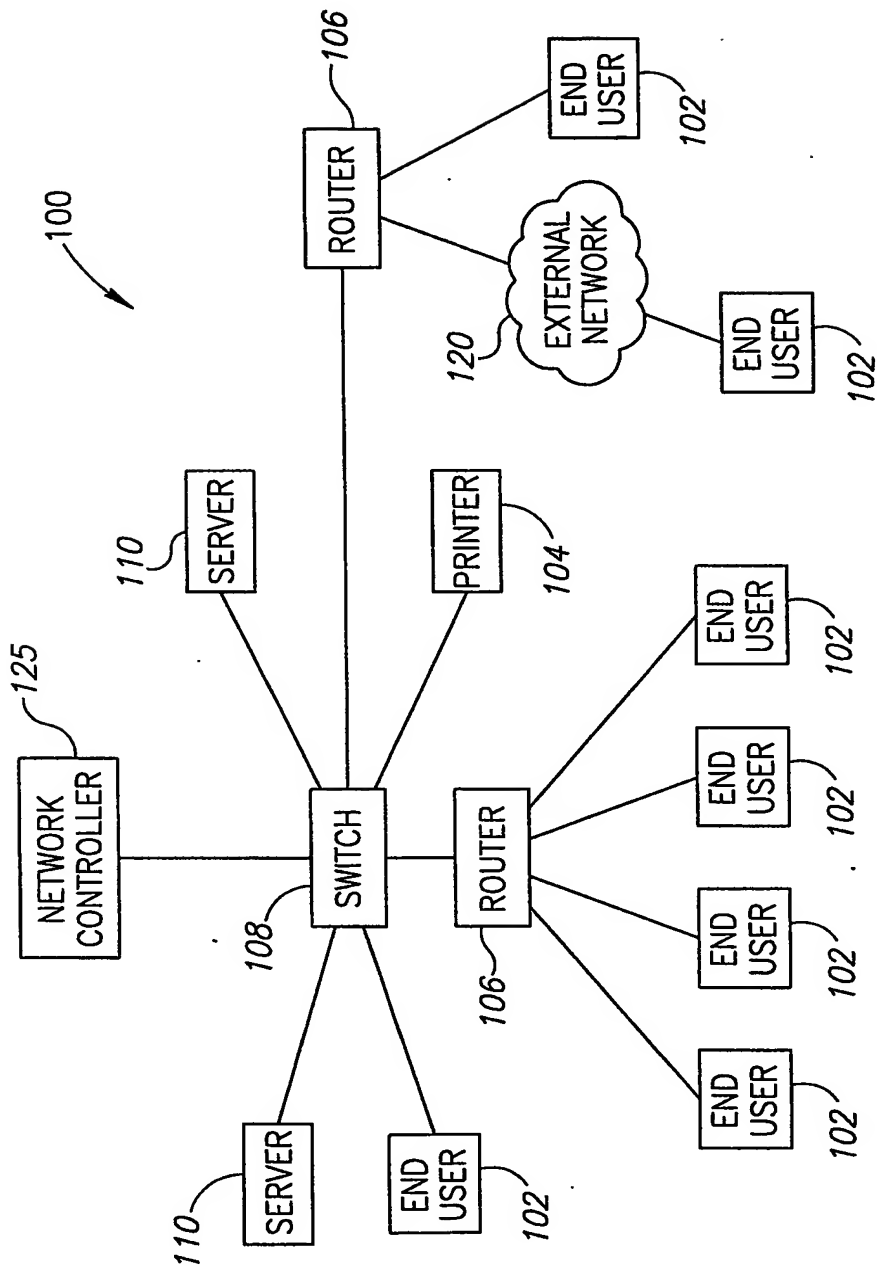


FIG.1

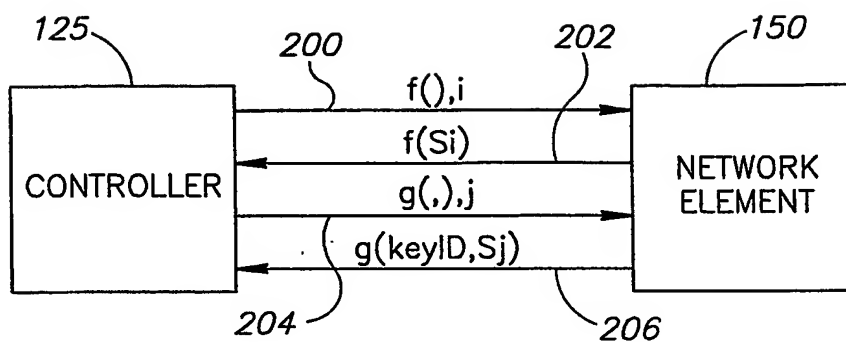


FIG. 2

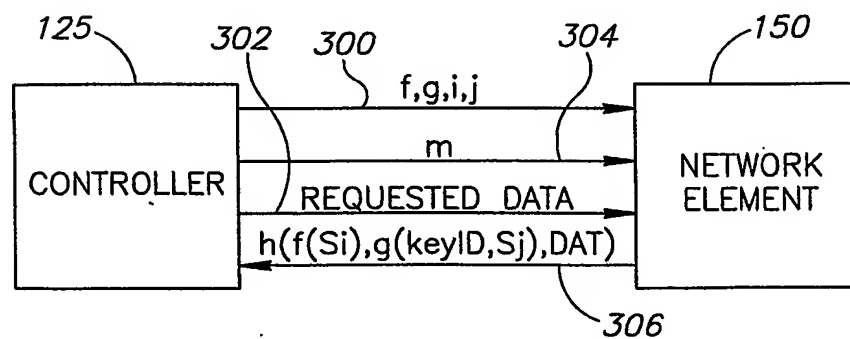


FIG. 3

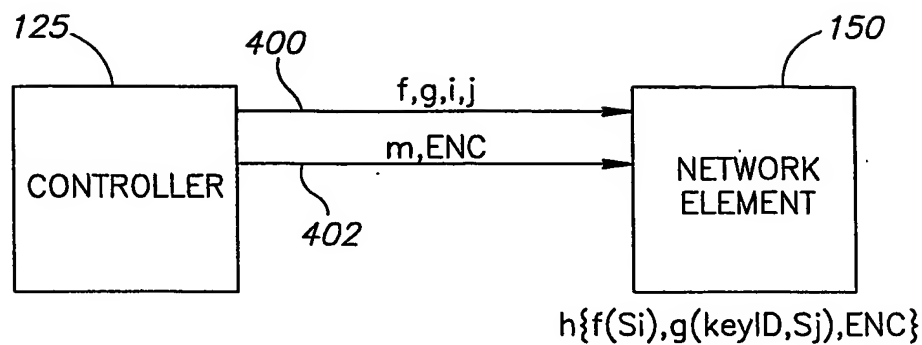


FIG. 4

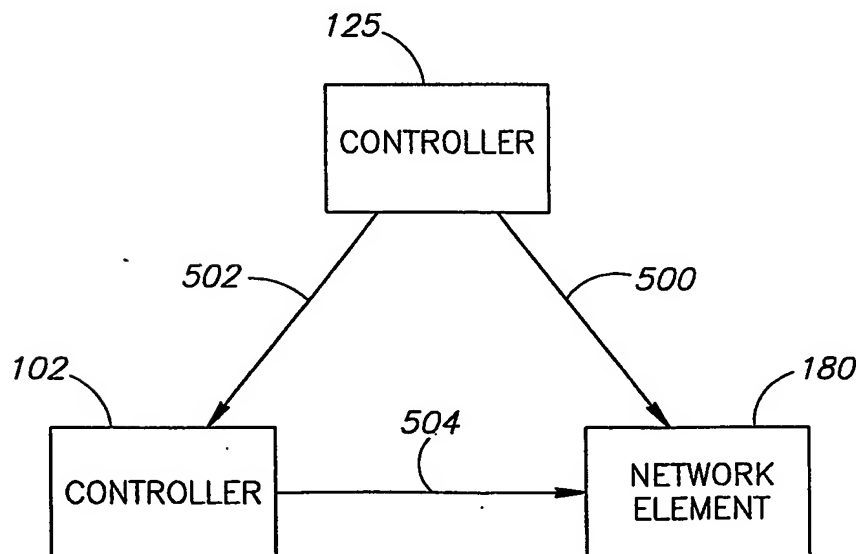


FIG. 5

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/IL04/000922

International filing date: 06 October 2004 (06.10.2004)

Document type: Certified copy of priority document

Document details: Country/Office: IL
Number: 158309
Filing date: 08 October 2003 (08.10.2003)

Date of receipt at the International Bureau: 23 November 2004 (23.11.2004)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.